Secretary of State
Oregon Audits Division

Public Employees Retirement System

Severe Deficiencies in Disaster Recovery Program and Insufficient Information Technology Planning Pose Substantial Risks to Beneficiaries and the State

October 2018
2018-32

Secretary of State Dennis Richardson
Audits Division Director Kip Memmott

This page intentionally left blank

Secretary of State
Audit Highlights

October 2018

Public Employees Retirement System

Severe Deficiencies in Disaster Recovery Program and Insufficient Information Technology Planning Pose Substantial Risks to Beneficiaries and the State

Report Highlights

The agency charged with administering the Public Employees Retirement System, or PERS, should improve Information Technology (IT) strategic planning efforts to ensure that IT investments return the most value and minimize risk. Additionally, PERS should immediately correct deficiencies with existing disaster recovery plans so the agency can effectively respond to catastrophic events that would prevent the use of existing IT hardware and software. PERS is working to update current plans and implement a recovery site, but a more urgent effort is needed.

This audit includes an assessment of critical security controls and the agency's IT security management practices. PERS should improve security management roles and training, as well as correct weaknesses in inventory management, configuration change management, vulnerability management, and controlling administrative accounts.

Background

PERS has over 365,000 members and is responsible for administering employee pension programs for state agencies as well as approximately 900 local governments. PERS provides $310 million in retirement benefits each month. The agency's Information Services Division provides PERS with information technology, such as pension benefit calculation software, to support agency operations.

Purpose

The purpose of this audit was to determine whether PERS could improve IT security and IT strategic planning efforts and to assess the agency's preparedness to restore critical IT systems in response to a disaster.

Key Findings

PERS's IT strategic planning lacks sufficient detail to help ensure IT investments return the most value, pose the least amount of risk, and are completed timely. Insufficient planning has contributed to mismanagement of some agency initiatives.

While PERS has identified a method to issue most pension payments in the event of a disaster, it has not fully addressed changes in payment processing by the Oregon State Treasury. The agency's disaster recovery plans pose serious risks because they are insufficient to restore critical IT systems. Furthermore, the agency has not tested those plans and has not yet complied with legislative mandates to acquire an alternative recovery site and improve disaster recovery planning. The agency's strategy to re-issue the prior month's payments poses risk of benefit payment errors and has never been tested.

Recommendations

Our report includes ten recommendations to PERS to implement improved IT strategic planning and to take immediate action to remedy weaknesses in its disaster recovery plans. In addition, we make six recommendations to PERS and the Office of the State Chief Information Officer related to Critical Security Controls.

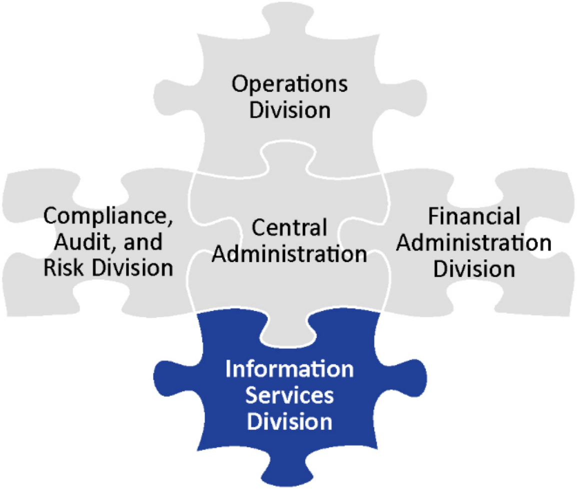
PERS agreed with all of our recommendations. The agency's response can be found at the end of the report.

Introduction

Most state and local government employees in Oregon participate in the Public Employees Retirement System, or PERS, a pension program administered by the state agency of the same name. PERS relies on several Information Technology (IT) systems to maintain payroll records, manage member accounts, and distribute funds to beneficiaries. This collection of systems is known as the Oregon Retirement Information Online Network.

The purpose of this audit was to determine if PERS can improve IT security and IT strategic planning practices in order to maximize the value of IT investments and minimize the risks of acquisitions. The audit's purpose was also to determine whether PERS can timely recover its IT systems in the event of a disaster.

Public Employees Retirement System


Operations Division
Compliance, Audit, and Risk Division
Central Administration
Financial Administration Division
Information Services Division

PERS provides pension benefits to state and local government employees

PERS is overseen by a five-member board.[1] The board hires an executive director to manage the agency's daily operations and its staff of about 375. As an executive branch agency, PERS also receives oversight from the Oregon Legislature, the Department of Administrative Services, and the Office of the State Chief Information Officer. PERS works closely with the Oregon State Treasury and Oregon Investment Council to manage the PERS trust fund. The agency has offices in Tigard, Tualatin, and Salem. PERS is organized into five distinct divisions:

- Central administration develops agency strategy, manages legislative and stakeholder relationships, and provides executive oversight of the agency;
- Information Services provides IT to enable agency business operations to be accomplished efficiently and effectively;
- Operations processes retirement applications and answers member and employer questions;
- Financial administration provides accounting, budgeting, and other administrative functions; and
- Compliance, Audit, and Risk oversees policy analysis, internal audit, business continuity planning, and information security and risk.

[1] PERS board members are appointed by the Governor to three-year terms. Three board members must be non-members with management or investment experience, one is an employer representative, and one represents employees and retirees.

The Information Services Division is made up of three sections: Technical Operations, Enterprise Applications, and Enterprise Content Management. Technical Operations administers, implements, and manages the day-to-day operations of PERS IT infrastructure. Enterprise Applications designs, develops, and tests enhancements to PERS's core systems. Enterprise Content Management is responsible for scanning all incoming mail as well as PERS's archival collection of microfiche film. The Information Services Division spent approximately $15 million in Fiscal Year 2017. Of that, approximately $7 million was spent on salaries and benefits for about 70 staff and about $4 million was paid to IT contractors.

PERS serves hundreds of thousands of Oregonians

PERS serves approximately 900 public employers in Oregon including schools, cities, counties, and state agencies. PERS provides pension programs for approximately 365,000 (about 95%) state and local government employees in Oregon. In addition to serving current and former public employees, PERS also works closely with members of their families and other designated beneficiaries. There are three benefit programs – Tier 1, Tier 2, and the Oregon Public Service Retirement Plan (OPSRP). See Figure 1 for a breakdown of PERS membership by pension program.

Figure 1: Hundreds of thousands of Oregonians are served by PERS

	PERS Tier 1	PERS Tier 2	Oregon Public Service Retirement Plan
Active member[2]	24,528	37,097	111,680
Inactive member[3]	14,037	15,692	15,980[4]
Receiving benefits[5]	125,344	12,234	3,437
Total	163,909	65,023	131,097

Source: Fiscal Year 2017 Comprehensive Annual Financial Report

PERS has a major impact on Oregon's economy. It directly impacts over 140,000 members, who receive approximately $310 million in total monthly payments. Additionally, each month the state and federal government receive approximately $20 million and $35 million, respectively, from PERS in associated tax withholdings on behalf of PERS beneficiaries. These benefit payments also indirectly impact the state economy through job creation. A 2017 study by PERS found the agency has a $3.9 billion impact to Oregon's economy.[6] About 1 in 60 dollars spent in Oregon is tied to PERS payments.[7]

Legislative pension reforms intended to contain costs added complexity and risks to PERS's operations

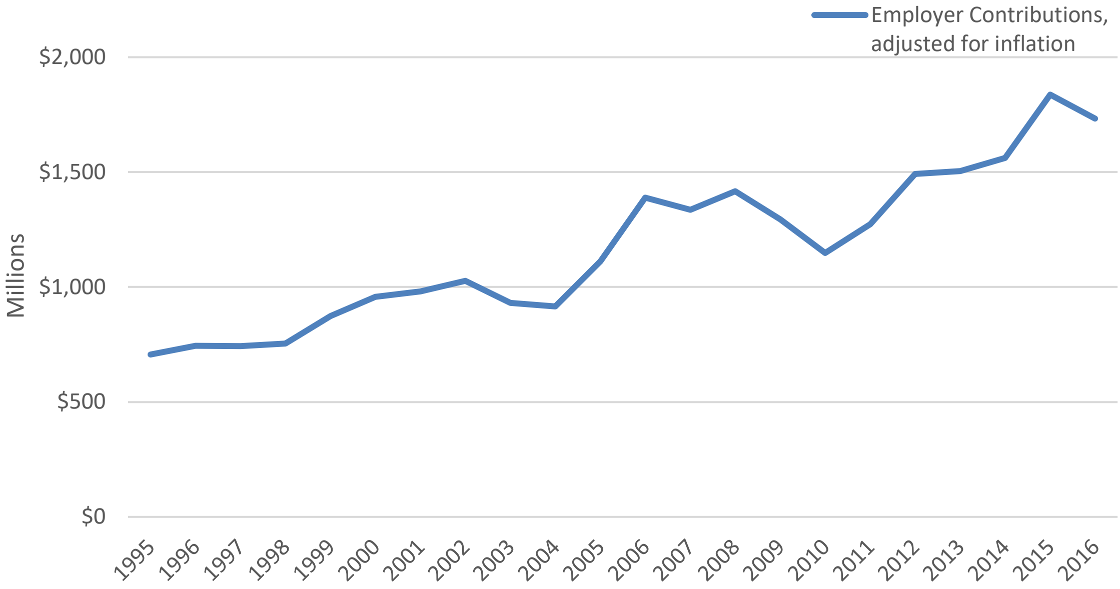
The Legislature has made several changes to PERS benefit programs in an attempt to lower pension costs paid by employers to fund the system, see figure 2. One of the biggest changes was to eliminate new membership in the defined benefit plans known as Tier 1 (1996) and Tier 2 (2003). Those programs provided more generous benefits than OPSRP, the only program

[2] An active member is currently employed in a PERS qualifying position in state or local government and has completed a six-month waiting period.
[3] An inactive member was previously an active member employed in a PERS qualifying position in state or local government.
[4] 11,795 inactive OPSRP members are not eligible for refund or retirement.
[5] This includes individuals who have opted to withdraw their account balances in a lump sum payment rather than receive a monthly payment.
[6] *Economic Impact Study Oregon Public Employees Retirement System* November 2017.
[7] The U.S. Bureau of Economic Analysis estimates the size of Oregon's economy to be roughly $236.2 billion in 2018.

available to new hires as of 2003. OPSRP is a hybrid pension system that combines a defined benefit and defined contribution plan.[8]

Pension reforms made in 2003 resulted in the creation of a defined contribution plan called the Individual Account Program (IAP). A percentage of an employee's salary goes into an account for that employee. Given that PERS was required to implement this program in only four months, it sought assistance from a third-party administrator. The administrator continues to provide a number of services to PERS, such as making disbursements from a member's IAP account when funds are withdrawn. PERS pays over $2 million per year for these services.

Figure 2: Employer contributions to PERS have grown even with some cost containment reforms



Source: PERS: By the Numbers report (2017) and Bureau of Labor Statistics Consumer Price Index data

Oregon Supreme Court rulings overturning some pension reforms required changes to IT systems

Oregon Supreme Court cases have had a significant impact on the way PERS administers pension programs requiring multiple alterations to the agency's IT systems. *Strunk v. Public Employees Retirement Board (2005)* and *City of Eugene v. Public Employees Retirement Board (2005)* related to several legislative changes made in 2003 and PERS benefit calculations. The Oregon Supreme Court allowed some reforms while ruling others unconstitutional and concluded that PERS overpaid some members based on inaccurate account crediting. A more recent case, *Moro v. Oregon (2015)*, overturned most of the 2013 legislative reforms that changed the pension benefits paid to certain members of PERS by limiting the cost of living adjustment and eliminating a tax offset for out of state retirees. While allowing for the tax offset to be eliminated, Oregon's Supreme Court ruled that changing to a progressive cost-of-living adjustment for benefits earned before the reform violated the terms of the contractual agreement between the State of Oregon and PERS members. These examples are just a few of the court cases that have significantly impacted PERS over the years.

Each legislative change required PERS to make changes to how their IT systems operate. When legislative reforms were subsequently overturned, some work-in-progress had to be abandoned and already implemented changes needed to be re-worked to undo the portions affected by the

[8] A defined benefit plan guarantees a specific benefit at retirement, while a defined contribution plan guarantees a specific contribution to a retirement account that is subject to market returns.

court cases. According to PERS, these changes also strained the IT capacity of the agency and did not allow foundational IT programs to progress as planned.

PERS's critical IT systems are difficult to manage and missing needed functionality

In the late 1990s, PERS began early planning efforts to replace a legacy IT system built during the 1980s known as the Retirement Information Management System. A report by PERS noted this legacy system was no longer able to keep up with increased customer demands and required hundreds of hours of programming to address legislative changes to the pension system that were becoming increasingly frequent.[9]

In 2001, PERS requested additional funding to hire staff to plan a replacement system. The Legislature, concerned about PERS's ability to manage a project of this size, ordered the agency to stop planning efforts and coordinate with legislative and executive branch oversight bodies before moving forward with the replacement system. The Legislature instructed PERS to use existing resources and reduced the budget for the replacement project to just $1.

PERS engaged with the oversight bodies and obtained funding for the replacement system in 2002. The project was rolled out over several phases with the project completed in 2010. PERS is currently exploring options to replace the current system because the system is difficult to modify and does not perform all needed functionality.

Recent concerns with PERS's information security vulnerabilities and disaster recovery planning spur executive and legislative branch action

In 2015, the Legislature instructed PERS to conduct a detailed health check and risk assessment of the agency's disaster recovery and business continuity environment due to concerns raised during the budget process. The Legislature restricted the agency's access to approximately $1.58 million in approved funding for disaster recovery efforts until the concerns were addressed.

In April 2016, the Governor's Office informed PERS that it was putting a pending budget request on hold due to concerns related to management of information security risks. According to a letter sent by the Governor's Office, PERS had not taken enough action to address concerns raised by the Legislature. In addition, the Governor's Office was concerned that PERS had neglected to share an independent IT security assessment during the 2016 budget deliberations. That security assessment identified a number of critical security vulnerabilities that put thousands of Oregonians' data at risk.

The Office of the State Chief Information Officer and Legislative Fiscal Office issued a joint memorandum to PERS following the letter from the Governor's Office. PERS was instructed to address 16 items critical to information security and disaster recovery by June 2017. In September 2017, the Office of the State Chief Information Officer noted that PERS had completed five of the 16, with 11 more complex items still needing attention. In September 2018, PERS updated the legislature on their remediation status and the agency's intent to complete the remaining items by the end of the 2017-19 biennium.

In June 2017, the Legislature again instructed PERS to respond to several security and disaster recovery issues. One related to developing and implementing a cybersecurity program and another related to the status of the ongoing Individual Account Program project. The Legislature also directed PERS to perform a comprehensive feasibility study on moving computing resources and operations to the State Data Center operated by the Department of Administrative

[9] *The Oregon Public Employees Retirement System History The First 60 Years*

Services. In addition, the Legislature directed PERS to develop an industry-standard Disaster Recovery Program, Business Continuity Program, and disaster recovery warm site.[10]

Our audit focuses on IT strategic planning practices, disaster recovery capabilities, and an assessment of IT security management and select critical security controls.

[10] A warm site is a facility with space, basic infrastructure, and all required equipment installed to support recovery of operations.

Objective, Scope, and Methodology

Objective

We had two objectives for this audit. The first was to determine whether PERS can improve IT strategic planning practices in order to maximize the value of IT investments and minimize the risks of IT acquisitions.

The second was to determine whether PERS can timely recover their information systems in the event of a disaster.

In addition to the two objectives, we reviewed PERS's IT security management program to determine the extent to which PERS has implemented appropriate security controls.

Scope

Our audit scope included IT strategic planning, IT resource management, IT portfolio management, disaster recovery, and IT security controls.

Methodology

To complete our audit objectives, we conducted interviews with department personnel and external stakeholders, observed department operations, anonymously surveyed key business managers, reviewed budgetary records from 1999 to 2018 and financial records from 2015 to 2018, and examined available system documentation. We also evaluated or tested:

- Policies, procedures, and plans governing agency and IT strategic planning, including portfolio management, resource management, and business-IT alignment;
- Policies, procedures, and plans for disaster recovery, offsite backup, and establishing an alternative site;
- Policies, procedures, and plans for cybersecurity.

To identify generally accepted control objectives and practices for information systems, we used the ISACA "COBIT," the United States Government Accountability Office's publication "Federal Information System Controls Audit Manual," the Center for Internet Security® publication "The CIS Critical Security Controls™ for Effective Cyber Defense v.6.1,"[11] the State of Oregon's "Statewide Information Security Standards March 2017" and International Standard ISO/IEC 27002 Second edition 2013-10-01 "Information Technology – Security Techniques – Code of practice for information security controls."

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We sincerely appreciate the courtesies and cooperation extended by officials and employees of PERS during the course of this audit.

[11] The Center for Internet Security, a 501(c)(3) non-profit, can be reached at controlsinfo@cisecurity.org

Audit Results

PERS should improve IT strategic planning efforts to ensure that IT investments return the most value and pose the least amount of risk to the agency and the employers whose contributions fund the administration of the pension program. Existing IT planning efforts are inadequate to enable timely completion of the agency's strategic objectives. PERS should also implement a system to track staff time spent on various tasks to enable effective IT planning.

Additionally, PERS should immediately correct deficiencies in existing disaster recovery plans so the agency can effectively respond to catastrophic events that would prevent the use of existing IT systems. The agency has not tested current disaster recovery plans and lacks an alternative recovery site. PERS is making progress to update current plans and implement a recovery site, but a more urgent effort is needed.

PERS needs to improve IT strategic planning, implement portfolio management, and better align its IT and business needs

Organizations should create an enterprise strategic plan that outlines strategic goals and objectives. Once an enterprise strategic plan has been developed, organizations that rely on IT should also develop an IT-specific strategic plan that outlines how technology will be leveraged to accomplish the objectives within the enterprise plan. The IT plan should document how IT optimizes value to the enterprise, how IT investments are managed, and the risk exposure relating to technology. The plan should be developed in cooperation with relevant stakeholders to ensure the goals of the enterprise are accurately captured.

Key Elements of IT Strategic Planning

1. Detailed written plan
2. Resource management
3. Portfolio management
4. Business-IT alignment

A critical element of IT strategic planning is managing investments through portfolio management, which is a systematic process for managing IT investments, projects, and activities. Portfolio management enables an organization to develop realistic objectives and measures for the IT strategic plan.

Portfolio management allows an organization to understand where resources are being applied so it can measure effectiveness and objectively evaluate how successful it is in achieving strategic goals and objectives. This includes measuring and tracking where staff time and financial resources are being applied. This understanding allows an organization to identify both how much effort is spent maintaining current systems as well as its capacity for taking on new projects to enhance IT systems. Portfolio management also provides an organization with a clearly defined scope of work.

Existing IT strategic plan lacks sufficient detail

PERS issued a formal strategic plan for 2015-2020, with a recent refresh for 2018-2023. Within the enterprise plan are three IT-focus areas. These focus areas, while important for defining the enterprise's priorities, do not provide the level of detail needed to achieve the agency's strategic IT goals.

> "Oregon PERS's new Chief Information Officer quickly realized that his division spends a lot of money, but that it doesn't really have a strategy for anything other than 'keeping the lights on.' The CIO wants to develop a long-term strategy to support the agency…"
> *- State of Oregon PERS HP ENVISION Summit 2014*

The agency's Chief Information Officer has taken steps to increase strategic planning efforts at the agency. For example, a day-long planning session was held in 2014 with senior managers and executives. One output of that meeting was a report that outlined the Chief Information Officer's vision of a long-term strategy to support the agency. Despite the good intentions and strong initial efforts, this vision was never realized and the intended strategy was never fully developed, although some elements of IT strategic planning were rolled into the enterprise strategic plan and some recent agency initiatives resulted from this planning session, according to PERS. A comprehensive document to highlight how IT will deliver value by managing investments geared towards strategic objectives remains to be completed.

A well-defined IT strategic plan should also identify the resources needed to achieve the objectives. Human capital is one of PERS's most important resources. During the course of this audit, multiple employees noted concerns about PERS recruiting and retaining IT staff. PERS has not defined within their planning documentation the skills and capabilities employees need to possess, nor has the agency defined training plans to ensure staff are sufficiently trained. In 2014, PERS developed an inventory of staff knowledge; however, these documents have not been regularly updated nor do they document the agency's need for specific skills and capabilities.

In 2017, the agency's internal auditor reported that the Information Services Division needed to develop a strategy to recruit and retain quality staff. This recommendation was accepted by PERS management who planned to implement it by December 2017; however, a detailed plan has not yet been developed and the new target implementation date is December 2018. Not knowing what skills are needed, or how to attract and retain those skills, hinders the agency's ability to implement projects and other strategic objectives in a timely manner. Furthermore, it creates reliance on contractors to obtain the skills needed to accomplish project objectives. For example, PERS partially relies on contractors to perform needed maintenance and enhancement to agency systems. Approximately one-quarter of the agency's IT budget is spent on contractors. In Fiscal Year 2017, payments to contractors totaled about $4 million.

Figure 2: PERS Needs to Improve IT Strategic Planning in Multiple Areas

Written Documentation	Resource Management	Portfolio Management	Business-IT Alignment
IT strategic goals and objectives are documented, but the plan lacks sufficient detail to help ensure IT investments return the most value, pose the least amount of risk, and are completed timely.	Financial tracking is sufficient for some major projects. No tracking of staff time spent on various tasks limits portfolio management and effective project budgeting.	Only major projects are managed, no comprehensive tracking of maintenance efforts.	Alignment was rated mediocre by PERS's Operations Division managers.

Insufficient planning hinders the effective use of approved funding and timely project completion

In 2015, the Legislature conditionally approved $1.58 million for PERS to improve its disaster recovery capability. According to the Legislative Fiscal Office, PERS made little progress to address the legislative directions that were part of the conditional approval, such as developing a prioritized action plan to address deficiencies in existing disaster recovery plans. However, due to the importance of making tangible progress towards improving the agency's disaster recovery program, the legislature released a portion of the funding in April 2017. Despite the release of this funding, PERS reported it was unable to spend any of the funds before the spending authority expired on June 30, 2017. PERS subsequently received $1.65 million in the 2017-19 biennium for disaster recovery-related purposes. Yet PERS has been unable to move the initiative forward. As of July 2018, only $22,000 has been spent on a consultant's report making recommendations to PERS about potential disaster recovery solutions.

A number of other IT projects in recent years have not been completed as planned. The Individual Account Program (IAP) project is one example. The 2003 pension reforms resulted in the creation of the IAP, but given that the pension reforms required implementing a new pension program in only four months, PERS sought assistance from a third-party administrator. The administrator, which has been under contract since that time, provides a number of services to PERS to enable the administration of the IAP. For example, the administrator makes disbursements from a member's IAP account when funds are withdrawn. PERS pays over $2 million per year for these services.

In 2013, PERS sought to bring the administration of the IAP fully within PERS, allowing the agency to save millions per year in fees it otherwise would have paid to the third-party administrator. The initial cost estimate for this IT project was just over $2 million, providing a positive return almost immediately if the project succeeded and stayed on budget. The Legislature, recognizing the value of bringing those services in-house, approved the initial request. The project was estimated to be completed by June 2017.

However, PERS did not complete the project, due in part to a decision by the Oregon Investment Council who is responsible for investment of all State of Oregon funds including the Oregon Public Employee Retirement Fund. The council decided to invest IAP accounts in Target Date Funds, which are funds grouped by a member's age and that automatically adjust to more conservative investments over time. This decision was made because of concerns about employees nearing retirement being exposed to the risk of a stock market crash — concerns that were raised as early as 2011, according to the Legislative Fiscal Office. In 2018, the Legislature declined to authorize additional funding due to growing project costs, implementation issues, and changes to the scope of the project that would no longer result in the initial estimated savings. As a result, after several years of work and over $4 million spent, it is unclear if the agency can achieve the intended savings of over $2 million per year as IAP administration continues to be outsourced.

Stronger planning may have identified the risk of changes to the IAP and provided PERS the flexibility to successfully implement this project. Furthermore, the agency has experienced multiple legislative, administrative, and judicial decisions over the years that impacted its business. Those factors indicate that PERS should consider using a flexible approach during planning.

Disaster recovery efforts are another area that has seen minimal progress. Disaster recovery was identified as an agency priority in 2014, but even with ongoing agency efforts, few items have been completed to address deficiencies with the agency's disaster recovery plan since that time. The agency still lacks a detailed recovery plan, has not provided adequate training to staff, has not tested the plan, has not determined whether it can restore its critical files and does not have an alternative site available for use in the event of a disaster.

Lack of portfolio management limits the agency's ability to meet strategic objectives

PERS is working on multiple projects to enhance current systems and to address weaknesses in cybersecurity and disaster recovery. Even so, staff told us they spend a significant amount of time just to maintain existing IT systems. Organizations should have a good understanding of where their investments of both staff time and financial resources are being applied. However, PERS management is not monitoring or managing time spent on IT tasks or staff workloads.

PERS only tracks staff who are assigned to key projects, with smaller projects and maintenance efforts not being tracked at all. Staff reported maintenance efforts take up a considerable portion of their day-to-day tasks. Without understanding the time requirements for someone to complete current tasks, or the time they have available to take on new projects, PERS cannot proactively manage its resources or projects.

PERS managers noted that when projects fall behind schedule, they reactively seek out additional staff to help on the project. Although reprioritizing resources can be an effective way to keep key projects on schedule, it is not a strategic practice without considering the organization's other projects and existing workloads. Because PERS does not track staff time, it is not possible to ensure resources are prioritized towards the most critical tasks.

Additionally, assigning staff to a project might not contribute significantly to its completion if the staff is unclear as to their specific role and responsibilities and, therefore, spend little or no time on the project. For instance, one employee told us they were informed they were helping with the disaster recovery project by a PERS manager, but they did not know their specific responsibilities or how to prioritize the new assignment with their many other responsibilities.

The lack of tracking also prevents PERS from gaining valuable insights on how much staff time will be needed on future projects that have similar scopes. This makes it difficult for the agency to adequately predict the timeframes of projects or strategically apply resources to meet the agency's goals.

Furthermore, some IT staff is managed outside the control of the Information Services Division. A group of 5 Information System Specialists in the Operations Division develop tools and workarounds for missing functionality within existing IT systems. These developers report to a manager in the business unit, not the PERS Chief Information Officer. Although these developers collaborate with the Information Services Division, having developers outside the direct control of the Chief Information Officer increases the risk that IT resources will not be strategically managed and can lead to duplicative efforts or the business unit developing tools that are not aligned with the agency's goals. We also found the developers in the business unit did not always follow appropriate access management practices. As a result, the business unit reported they were unable to access some software code after a developer left PERS employment.

The alignment between operational needs and IT planning and actions needs to be strengthened

Operations and IT are aligned when organizational needs are met through the strategic investment of IT resources, when IT strategic goals are designed to help support the strategic goals of PERS, and when IT delivers value to the organization. Alignment between operations and IT should be a collaborative process driven by executive leadership with feedback from agency stakeholders, such as front line staff and managers.

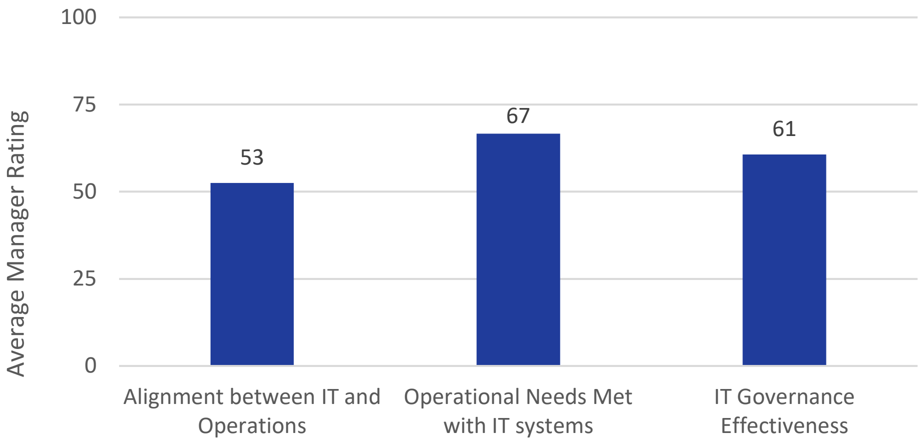
Survey Guidance for Operations-IT Alignment Rating

1 = no alignment
25 = minimal alignment
50 = some alignment
75 = mostly aligned
100 = perfectly aligned

We used an anonymous survey to gauge how Operations Division management perceived the Information Services Division's alignment with their business needs, such as being able to process various types of retirement applications. For the survey, we contacted 12 senior PERS business managers from the Operations Division whose staff interact constantly with critical PERS IT systems. The 10 managers who responded to the survey identified a number of potential opportunities for improvement.

We asked the managers to assess how well the Information Services Division was meeting goals in three areas — Business-IT alignment, business needs being met, and the effectiveness of IT governance. We asked them to provide a rating on a scale of 1 to 100, with a low score indicating the division is doing poorly and a high score indicating it is doing well. As noted in Figure 3, managers assessed the Information Services Division between 50 and 75 in all three areas. Although this survey tool is not a definitive measure, it shows that Operations Division managers saw an opportunity to strengthen the alignment with the Information Services Division. PERS's new executive director believes the agency's alignment between the Operations Division and Information Services Division is stronger than is shown by this survey.

Figure 3: Survey results of senior PERS managers highlights opportunities for improvement



Other questions included in the survey addressed collaboration with the Information Services Division and knowledge of IT strategic direction. Only three of the 10 surveyed managers viewed the Information Services Division as collaborative. No manager could identify all three focus areas for IT within the enterprise strategic plan, although most identified one element. These results indicate the potential to increase communication and outreach to key stakeholders within the organization.

In addition to the quantitative measures, we asked managers to respond to open-ended questions about business alignment, meeting business needs, and IT governance. Generally, managers highlighted areas of concern such as poor alignment between the divisions or lack of collaboration. Of the 24 open-ended responses, we categorized two as positive, five as neutral, and 17 as negative.

Selected survey responses of PERS managers

- There seems to be a disconnect between IT and Business. This, from my perspective, is due to IT having a hard time understanding the language business speaks. By not understanding business processes, it is more difficult to meet the needs of the business IT is meant to support.
- It seems mostly [the Information Services Division] is telling business what they can't do, vs. working together to solve problems or make process improvements.
- Competing priorities and too many projects get in the way.
- I believe we have an issue facing our agency, it seems that our skills have not kept up with technology, as I see more and more of our resources being spent on contractors for even system maintenance.
- [The Information Services Division] has been very collaborative and understanding of the needs of our business. They have been open to working together, and that has allowed for what I see as 'forward progress' toward actual solutions.

External factors such as legislative changes, court rulings, and administrative decisions put pressure on PERS

PERS is responsible for managing a complex retirement system that has gone through many changes and reforms over the years. Each change has the potential to create additional layers of complexity, making it all the more difficult to administer the pension program. One benchmarking firm ranks PERS among the most complex retirement programs in the country. [12] The system's reported complexity stems in part from operating three different pension tiers of benefit accruals, each with multiple formulas to calculate benefits and multiple payment options available to beneficiaries, as well as the Individual Account Program which has also increased in complexity since its inception.

Two significant legislative reforms within the past 20 years have required significant implementations or modifications of PERS's IT systems. Furthermore, both reforms were subject to legal actions with many elements of the reforms being overturned after the agency had already spent time and resources to modify their IT systems. This forced the agency to scrap already completed work and make further revisions to their systems. In addition to legislative reforms, PERS noted that the state's budget process provides limited flexibility given the long lead times required to submit budget requests.

A recent administrative decision by the Oregon Investment Council also impacted PERS's ability to complete a project. In 2017, the Oregon Investment Council changed how IAP funds were invested. This move affected PERS's project to bring administration of the IAP in-house. In the end, the IAP project was canceled, in part due to the administrative decision by the Oregon Investment Council.

All of these external factors place greater importance on strong strategic planning. Strong planning can provide implementation flexibility as more risks are identified early on and addressed before they create critical dependencies. For example, PERS may have been able to identify the risk posed by investment changes and developed an IT solution for the IAP project that would have been compatible with investment approaches such as Target Date Funds. Portfolio management will also allow PERS to ensure that sufficient resources are being applied to critical initiatives like disaster recovery planning efforts.

PERS is not prepared to restore critical systems in the event of a disaster

The agency's existing capability to respond to a disaster is hampered by the lack of a detailed disaster recovery plan and a viable alternative data center site. PERS has not tested critical elements in existing disaster recovery plans. Without adequate testing, the agency does not have assurance that its plan to restore critical IT systems will work. PERS requires IT systems to effectively manage their pension programs. Without those systems, payments to beneficiaries and other critical business processes are at risk.

Industry best practices call for strong disaster preparedness

Organizations, especially those relying heavily upon IT, should develop strong disaster recovery plans to ensure they are able to continue operating after a disaster occurs resulting in the inoperability of critical resources. Disaster recovery planning begins with identifying potential business interruption events, such as an earthquake, flood, fire, or other potential disruptions

[12] 2017 report by CEM Benchmarking incorporated

caused by humans. If an organization understands what risks they face, they can begin to formulate a strategy for how to deal with and mitigate their impact.[13]

Disaster recovery plans outline the steps necessary to help an organization recover from a variety of potential service disruptions. The goal of the plan is to help the agency minimize the possible occurrence of disruptions or reduce disruptions to an acceptable duration of time. The plan is also a foundational document for how to get critical computer systems restored and working after they have been disrupted.

To ensure that data is protected from loss during a disaster, organizations should back up files and store them in a remote location at a sufficient distance to escape any damage from a disaster occurring at the main site. Management should ensure that offsite arrangements are periodically assessed, ensure compatibility of hardware and software to restore archived data, and periodically test existing backup data and infrastructure. Testing allows an organization to identify gaps in procedures and other documentation that may prevent the restoration of information systems. It also allows for the identification of any issues with hardware or software that could prevent successful restorations.

In addition, entities that cannot perform their critical business functions without their IT systems should consider having an alternative recovery site. An alternative recovery site is a backup set of IT infrastructure that can be made available in the event of a major disaster. This site should be far enough from the primary site to ensure that both the primary and backup systems do not become unavailable during the same event. In June 2017, the Legislature directed PERS to begin developing a warm site.

Different Types of Alternative Sites

Cold Site: A facility with space and basic infrastructure to support recovery of operations

Warm Site: A facility with space, basic infrastructure, and all required equipment installed to support recovery of operations

Hot Site: A facility with space, basic infrastructure, all required equipment, and all required software installed and running to support recovery of operations

Alternative sites are expensive because they duplicate IT investments

In order to develop a warm site, PERS will need to invest significant resources. Sites that require minimal time to restore services will essentially be a complete duplication of existing IT systems. It is costly to equip these sites by their very nature. Even sites without duplicated hardware are expensive, as the cost has only been delayed. Recovery still relies upon purchasing needed IT equipment. During certain disasters, needed equipment might not even be available for purchase.

Alternative sites may require a substantial investment, but they provide valuable insurance to organizations during major disasters. With a suitable alternative site, organizations can get back to operating their critical IT systems in just a few hours. Without one, an organization may never be able to recover, or be unable to do so in a timely and economical way.

The need for enhanced disaster recovery capabilities has been recognized by PERS since 2014

In 2014, PERS recognized the need for improved disaster recovery strategies, including obtaining a secure alternative site. The agency attempted to address these deficiencies by including disaster recovery as a strategic objective for IT within the 2015-2020 enterprise

[13] Disaster recovery is related with Continuity of Operations Planning, sometimes known as Business Continuity Planning, which was the subject of audit report no. 2018-03, "Office of Emergency Management: The State Must Do More to Prepare Oregon for a Catastrophic Disaster."

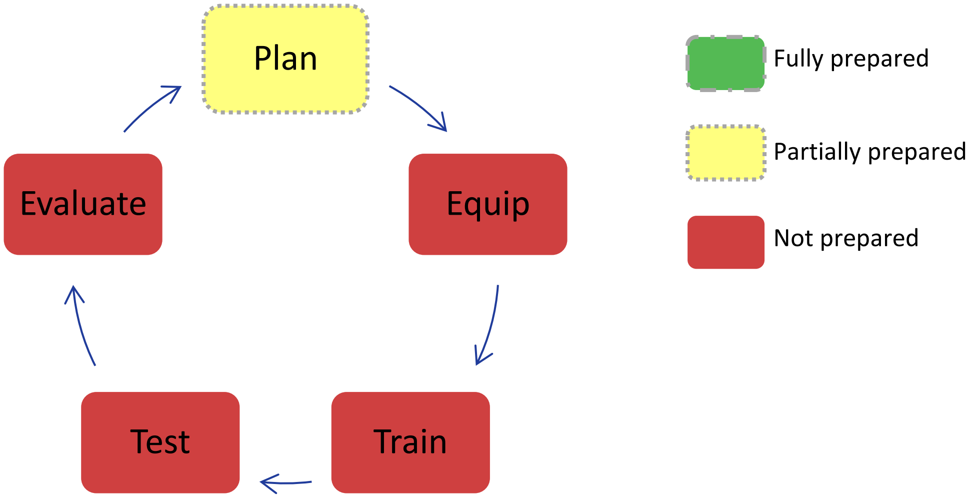
strategic plan. The goal was to develop and implement infrastructure to provide business continuity of the critical IT systems and to improve existing disaster recovery plans. The agency also set a goal of completing a full and complete disaster recovery test by 2020. The disaster recovery focus area in the enterprise strategic plan stated:

> The third IT focus area is disaster recovery. PERS does not currently have a secure off-site location for data recovery necessary to business continuity, nor the network equipment needed to rebuild systems and infrastructure. This goal is to develop and implement an infrastructure that will provide business continuity of the critical [Oregon Retirement Information Online Network] systems necessary to minimize the impact of any localized disaster on our members, employers, and staff.
>
> **Objective 1:** Define the technology infrastructure that is at risk in the event of a localized disaster and execute a strategy to restore that infrastructure
>
> ***Strategies***
>
> 1. Identify the critical management systems and supporting infrastructure necessary to meet the agency's business continuity requirements.
>
> 2. Develop a strategy to enable single sign-on functionality for the critical management systems.
>
> 3. Design and implement a virtual desktop infrastructure to support the agency's remote access requirements.
>
> **Objective 2:** Update the agency's Business Continuity Plan to align with disaster recovery strategies and infrastructure.
>
> ***Strategies***
>
> 1. Develop a strategy for deploying a back-up recovery site ("warm site") that would be used to provide access to core business systems and infrastructure.
>
> 2. Execute a complete and full disaster recovery test.

In February 2017, the agency drafted a formal disaster recovery plan and submitted it to the Office of the State Chief Information Officer for review and approval in September 2017. The Office of the State Chief Information Officer noted that further work was required to create a viable plan. Several modifications and additions have been made; however, these efforts appear to be reactive requests from various oversight bodies and the changes have sometimes been limited in scope. Even after receiving feedback that the current plan was inadequate, there was a period of four months where the plan had not been modified and then only minor changes were made.

Disaster recovery efforts require strong planning, equipping, training, testing, and evaluation to ensure the approach being used is effective to remediate the loss of service during a disaster. The status of these efforts at PERS are highlighted in Figure 4 and the following section.

Figure 4: Status of PERS's Disaster Preparedness



Source: Based on Federal Emergency Management Agency disaster preparedness guidance

Disaster recovery plans are incomplete and have never been tested

Although instructed by the Legislature in 2017 to develop an industry-standard Disaster Recovery Program and disaster recovery warm site, the agency's work towards improving disaster recovery capabilities remains incomplete. PERS has documented procedures and identified a plan to make pension payments to benefit recipients if critical systems are unavailable for less than 30 days. However, the plan to fully restore critical systems has been in draft since February 2017 and the agency does not yet have a warm site available. In addition, the draft plan includes only one possible disaster scenario and lacks sufficient detail for staff to be able to timely restore critical systems. Furthermore, agency staff have not received training related to the procedures or draft plan and no tests have been done to determine if the approach would be successful.

In the event of a disaster where PERS's critical systems become unavailable for less than 30 days, the agency's short-term plan is to contact the Oregon State Treasury and request reissuance of the prior month's pension payments. In theory, Treasury would be able re-process those prior payments with updated dates. The procedures for this plan have been documented, but they lack sufficient detail. In August 2018, PERS performed a successful tabletop exercise with the Oregon State Treasury to go over these procedures, but PERS has yet to fully test whether the electronic file can be re-processed in the way the agency intends. PERS has contracted with an external vendor to assist with the development, certification, and testing of their disaster recovery program, including a full test of their short-term plan.

In addition, the Oregon State Treasury recently kicked off a yearlong project to move payment processing to a third-party financial institution. Once complete, the Oregon State Treasury will not be able to assist PERS in reprocessing the prior month pension payments. This pending project and changeover has been communicated to PERS on several occasions over the last four years. The Oregon State Treasury indicated it will assist PERS in finding a viable solution as processes change, but no formal plan has been developed to ensure the new third-party financial institution will accommodate existing procedures.

The short-term plan also poses a significant risk of benefit payment errors. PERS issues over 800 lump-sum payments to individuals each year, averaging approximately $7.6 million dollars per month. The plan will require time-consuming reconciliation and collection processes to recover overpayments. For example, benefit payments would continue to be paid to any PERS beneficiary that passed away during the month prior to the disaster, likely resulting in an overpayment. In addition, the plan excludes payments that PERS would typically issue in a given month. For example, IAP retirement payments are excluded from existing disaster recovery plans. Lastly, new retirees would not receive benefit payments they are due, as they would not be on the prior month's pension file. According to PERS, the agency is willing to accept the risks involved with the short-term plan.

If the short-term plan fails, PERS may be unable to issue millions of dollars of payments in a timely fashion and there would likely be overpayments that would not be timely detected or collected. As a result, millions of dollars in monthly payments to PERS beneficiaries may be at risk of not being made timely or accurately.

Furthermore, the agency has not yet implemented a disaster recovery warm site to fully restore critical systems in the event that the primary location is unavailable beyond 30 days. Without an alternative site in place prior to a disaster, the recovery time for the agency will be significantly longer as they will need to work with a vendor to set up hardware and networking before restoring critical systems and data. After the computing infrastructure is in place, PERS will need to access backup files from their off-site location. PERS currently stores their off-site backup tapes with a vendor located only 1.5 miles from their headquarters.

Although the existing tape backup process is secure and well documented, the close proximity increases the risk that a major disaster, such as the Cascadia Subduction Zone Earthquake, could make both the primary systems and critical backup data unavailable. If this were to occur, PERS may not be able to restore critical systems to ensure payments can be made to its 140,000 beneficiaries beyond its 30 day short-term plan. PERS is currently engaged in a project to implement a new backup process where data will be stored remotely by a third-party using a cloud storage provider.[14] However, until this is implemented, there is little assurance that PERS would be able to timely recover critical systems in the event of a major disaster and the Legislative mandate to implement an off-site backup center remains unfulfilled.

Lack of attention from prior management contributed to slow progress on disaster recovery initiatives

A lack of management attention and prioritization of disaster recovery efforts have contributed to the current state of PERS's disaster recovery capability. Over the last several years, work on disaster recovery has often started and stopped with little continuity or sustained effort. In order to be prepared, sufficient dedicated staffing is needed to ensure that plans are continually refined and employees are trained.

Furthermore, the agency has not invested sufficient resources in its disaster recovery program in a timely manner. PERS recently reassigned staff to work on disaster recovery efforts, but provided little direction and did not clearly define roles and responsibilities. As of July 2018, years after identifying a need to improve the agency's disaster recovery program, PERS had expended only $22,000 — 1.3% — of the approximately $1.65 million in resources allocated to the agency to address deficiencies with disaster recovery.[15] PERS has indicated that spending will soon increase as current procurement efforts are finalized.

[14] A cloud storage provider offers the ability to store data in an off-site location owned by the service provider.

[15] The 2017-19 Legislatively Adopted Budget provided PERS $500,000 for disaster recovery programs and $1.2 million for disaster recovery warm site.

Critical Security Control Assessment

Cybersecurity Assessment

During this audit, we performed a review of the agency's IT security management program. The objective of this work was to determine the extent to which PERS has implemented an appropriate IT security management program, including the top five of the 20 security controls (CIS Controls™) published by the Center for Internet Security®.[16] Auditors interviewed agency staff, reviewed documentation, and performed limited control testing to assess whether management has established policies and implemented controls to stop cyberattacks that may target the agency.

PERS Security Management Program

At PERS, the security management program is a collaborative effort with Office of the State Chief Information Officer. The agency is responsible for the development, documentation, and implementation of a security management program. PERS's security plan is up-to-date and the agency is currently in the process of updating its security policies and standards; however, implementation of plan requirements is ad hoc and the newly implemented plan does not document clearly defined responsibilities. We found the agency generally lacks appropriate controls for implementing and monitoring security training, and for performing background verification for certain individuals accessing systems, including temporary employees and external third parties. In addition, the agency has not performed a security risk assessment since 2016. According to PERS, the agency will perform a new security assessment after remediation activities for the last assessment are completed. Performing such an assessment is typically a starting point for developing and modifying security policies and plans.

Security management is the foundation to security control and structure in an organization. Entities should have policies, plans, and procedures that describe the management program and cover all major systems, facilities, and applications.

Agencies should:

- periodically assess and validate risks;
- document and implement security control policies and procedures;
- implement and monitor effective security awareness trainings;
- remediate information security weaknesses; and
- ensure external third parties are adequately secured.

Without a well-designed program, security controls are likely inadequate; responsibilities may be unclear, misunderstood, or improperly implemented; and controls are at risk of being inconsistently applied, leaving the agency vulnerable to attacks.

Critical Security Controls

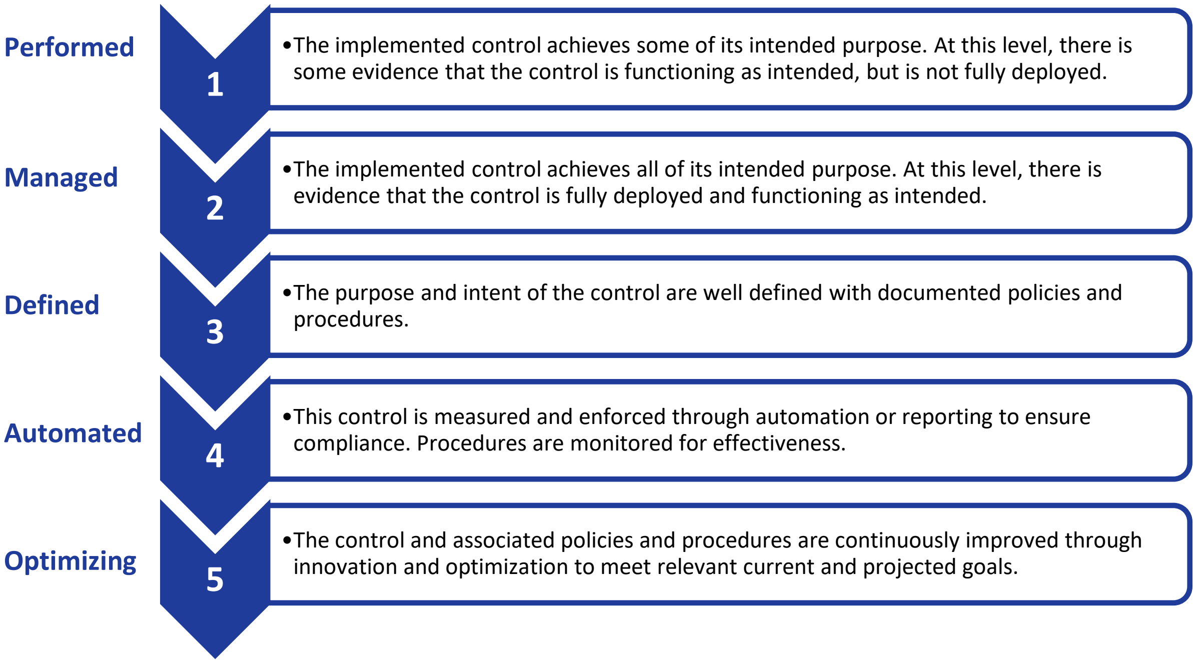
As part of the review, we assessed the agency's cybersecurity control environment capability. A capable control environment provides assurance that the agency has implemented foundational measures to mitigate common attacks against the agency's information systems. Cybersecurity experts generally agree that addressing only the top five controls of the 20 CIS Controls™ significantly reduces most of an organization's vulnerabilities. In addition to the CIS Controls™,

[16] Version 6.1, licensed under creative commons non-commercial no derivatives license

we used the Federal Information System Controls Audit Manual as IT security management criteria.

For this assessment, we evaluated the agency's cybersecurity control environment using an adapted version of the COBIT Capability Maturity Model. In a typical assessment using this model, a capability rating can only be achieved after the level below is fully achieved and each organization should set its target capability level based on its unique risks. Instead, we evaluated each sub-control against all five levels of the Model to provide an assessment of the agency's overall capability with more context and detail than would normally be assigned. For example, with this adapted version of the assessment, an agency may be shown to have defined policies addressing the control even if they have not actually implemented it.

Figure 5: Control Capability Maturity Model[17]



Performed 1
- The implemented control achieves some of its intended purpose. At this level, there is some evidence that the control is functioning as intended, but is not fully deployed.

Managed 2
- The implemented control achieves all of its intended purpose. At this level, there is evidence that the control is fully deployed and functioning as intended.

Defined 3
- The purpose and intent of the control are well defined with documented policies and procedures.

Automated 4
- This control is measured and enforced through automation or reporting to ensure compliance. Procedures are monitored for effectiveness.

Optimizing 5
- The control and associated policies and procedures are continuously improved through innovation and optimization to meet relevant current and projected goals.

Some maturity levels will not apply to select sub-controls due to their intended function. For example, to implement sub-control 1.3 requires automation. Therefore, it cannot be implemented at levels one and two. We indicate these with "n/a" on the following charts.

[17] Auditor created based on *COBIT 5 Business Framework* Capability Maturity Model, a recognized best practice in the IT industry.

CIS Control 1™: Inventory of Authorized and Unauthorized Devices

		Audit Results				
#	**CIS Critical Security Controls™, Sub-Controls v6.1** Inventory of Authorized and Unauthorized Devices	**Performed**	**Managed**	**Defined**	**Automated**	**Optimizing**
1.1	Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization's public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.	●	●	◐	●	○
1.2	If the organization is dynamically assigning addresses using DHCP, then deploy dynamic host configuration protocol (DHCP) server logging, and use this information to improve the asset inventory and help detect unknown systems.	●	○	◐	○	○
1.3	Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network.	n/a	n/a	◐	○	○
1.4	Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc. The asset inventory created must also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network.	●	●	◐	●	○
1.5	Use network level authentication via 802.1x to limit and control which devices can be connected to the network. The 802.1x must be tied into the inventory data to determine authorized versus unauthorized systems.	●	●	◐	●	○
1.6	Use client certificates to validate and authenticate systems prior to connecting to the private network.	●	●	○	●	○

○ = Not implemented ◐ = Partially Implemented ● = Fully Implemented n/a = Not Applicable

We evaluated the agency's processes to identify network devices, maintain an updated inventory of hardware devices, and control devices that can connect to the network. We found that PERS generally lacks formal policies in this area; however, it has implemented a number of automated controls to perform hardware inventory and blocks unauthorized devices from connecting to its network. For example, PERS recently implemented a system that automatically develops an inventory of authorized and unauthorized devices on the agency's network.

Any new device introduced to an agency's network may introduce vulnerabilities. Ensuring only authorized devices have access to information on the agency's network allows IT professionals to identify and remediate vulnerabilities by implementing proper security controls. However, without a clear understanding of which devices are on the network, the agency cannot ensure that proper controls are in place for those devices. Additionally, without an up-to-date inventory of authorized hardware, the agency may not identify unauthorized devices, which limits the agency's ability to prevent or detect unauthorized access to the network.

CIS Control™ 2: Inventory of Authorized and Unauthorized Software

		Audit Results				
#	**CIS Critical Security Controls™, Sub-Controls v6.1** Inventory of Authorized and Unauthorized Software	**Performed**	**Managed**	**Defined**	**Automated**	**Optimizing**
2.1	Devise a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified.	●	○	◐	◐	○
2.2	Deploy application whitelisting technology that allows systems to run software only if it is included on the whitelist and Protects execution of all other software on the system. The whitelist may be very extensive (as is available from commercial whitelist vendors), so that users are not inconvenienced when using common software. Or, for some special-purpose systems (which require only a small number of programs to achieve their needed business functionality), the whitelist may be quite narrow.	n/a	n/a	○	○	○
2.3	Deploy software inventory tools throughout the organization covering each of the operating system types in use, including servers, workstations, and laptops. The software inventory system should track the version of the underlying operating system as well as the applications installed on it. The software inventory systems must be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.	●	●	○	●	○
2.4	Virtual machines and/or air-gapped systems should be used to isolate and run applications that are required for business operations but based on higher risk should not be installed within a networked environment.	○	○	●	○	○

○ = Not implemented ◐ = Partially Implemented ● = Fully Implemented n/a = Not Applicable

We evaluated the agency's processes to document approved software, determine high-risk software, and identify software on the agency's systems. We found that while the agency has implemented some automated controls to inventory software, it generally lacks formal policies in this area. For example, PERS has recently implemented a new tool that automatically develops an inventory of software on agency hardware, but the agency does not use software whitelisting.[18]

The agency should maintain an inventory of software installed on their computer systems similar to the inventory of its hardware assets. Without a complete, accurate, and up-to-date list of the software that is authorized to be on the agency's systems, the agency cannot ensure effective controls are in place to protect software on the agency's information systems.

In addition to not being able to effectively safeguard authorized software, without an inventory of system software, the agency may be unable to identify unauthorized software on the agency's information systems, such as malicious software or software with known vulnerabilities. Attackers can exploit systems with malicious or vulnerable software to gain unauthorized access to the agency's data or disrupt the agency's operations.

[18] Software whitelisting is the practice of identifying a list of approved software to be installed on computer systems and restricting access installation to only approved software. Whitelisting reduces the risk of malicious software such as computer viruses or ransomware.

CIS Control™ 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

		Audit Results				
#	**CIS Critical Security Controls™, Sub-Controls v6.1** Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	**Performed**	**Managed**	**Defined**	**Automated**	**Optimizing**
3.1	Establish standard secure configurations of your operating systems and software applications. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.	●	○	○	◐	○
3.2	Follow strict configuration management, building a secure image that is used to build all new systems that are deployed in the enterprise. Any existing system that becomes compromised should be re-imaged with the secure build. Regular updates or exceptions to this image should be integrated into the organization's change management processes. Images should be created for workstations, servers, and other system types used by the organization.	●	●	◐	●	○
3.3	Store the master images on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible. Alternatively, these master images can be stored in offline machines, air-gapped from the production network, with images copied via secure media to move them between the image storage servers and the production network.	n/a	●	○	●	○
3.4	Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.	●	●	●	●	○
3.5	Use file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered. The reporting system should: have the ability to account for routine and expected changes; highlight and alert on unusual or unexpected alterations; show the history of configuration changes over time and identify who made the change (including the original logged-in account in the event of a user ID switch, such as with the su or sudo command). These integrity checks should identify suspicious system alterations such as: owner and permissions changes to files or directories; the use of alternate data streams which could be used to hide malicious activities; and the introduction of extra files into key system areas (which could indicate malicious payloads left by attackers or additional files inappropriately added during batch distribution processes).	n/a	○	○	◐	○
3.6	Implement and test an automated configuration monitoring system that verifies all remotely testable secure configuration elements, and alerts when unauthorized changes occur. This includes detecting new listening ports, new administrative users, changes to group and local policy objects (where applicable), and new services running on a system. Whenever possible use tools compliant with the Security Content Automation Protocol (SCAP) in order to streamline reporting and integration.	n/a	n/a	○	◐	○
3.7	Deploy system configuration management tools, such as Active Directory Group Policy Objects for Microsoft Windows systems or Puppet for UNIX systems that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals. They should be capable of triggering redeployment of configuration settings on a scheduled, manual, or event-driven basis.	●	●	○	●	○

○ = Not implemented ◐ = Partially Implemented ● = Fully Implemented n/a = Not Applicable

We evaluated the agency's processes to document and safeguard baseline configurations, deploy secure configurations, and monitor configurations on their network. We found that PERS generally lacks formal policies related to this control. PERS has implemented or partially implemented automated controls for all of the sub-controls. For example, the agency deploys secure configurations using a centralized process; however, those configurations can be modified by administrators and there is no process to monitor that activity. In practice, compromised machines are reimaged using secure configurations, but this process is not formally documented or monitored.

The agency should have processes in place to ensure hardware and software are securely configured. When agency management establishes a need for an information system, they should consider information security requirements. Default configurations may not align with business or security needs, and may leave the agency's systems vulnerable to attack. The agency should have configuration management processes in place that address implementing secure system control features at the initiation of the system life cycle. Furthermore, an organization should ensure configurations remain secure as modifications are made to the system. Configuration baselines should be documented so that agency personnel can effectively monitor actual configurations to ensure they align with established baselines. Also, policies and procedures should be in place that address how configuration baselines are managed.

CIS Control™ 4: Continuous Vulnerability Assessment and Remediation

		Audit Results				
#	**CIS Critical Security Controls™, Sub-Controls v6.1** Continuous Vulnerability Assessment and Remediation	**Performed**	**Managed**	**Defined**	**Automated**	**Optimizing**
4.1	Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk. Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project).	●	○	●	◐	○
4.2	Correlate event logs with information from vulnerability scans to fulfill two goals. First, personnel should verify that the activity of the regular vulnerability scanning tools is itself logged. Second, personnel should be able to correlate attack detection events with prior vulnerability scanning results to determine whether the given exploit was used against a target known to be vulnerable.	●	○	◐	◐	○
4.3	Perform vulnerability scanning in authenticated mode either with agents running locally on each end system to analyze the security configuration or with remote scanners that are given administrative rights on the system being tested. Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses. Ensure that only authorized employees have access to the vulnerability management user interface and that roles are applied to each user.	●	○	○	◐	○
4.4	Subscribe to vulnerability intelligence services in order to stay aware of emerging exposures, and use the information gained from this subscription to update the organization's vulnerability scanning activities on at least a monthly basis. Alternatively, ensure that the vulnerability scanning tools you use are regularly updated with all relevant important security vulnerabilities.	●	n/a	◐	n/a	○
4.5	Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe. Patches should be applied to all systems, even systems that are properly air gapped.	●	○	◐	◐	○
4.6	Monitor logs associated with any scanning activity and associated administrator accounts to ensure that this activity is limited to the timeframes of legitimate scans.	●	●	●	◐	○
4.7	Compare the results from back-to-back vulnerability scans to verify that vulnerabilities were addressed either by patching, implementing a compensating control, or documenting and accepting a reasonable business risk. Such acceptance of business risks for existing vulnerabilities should be periodically reviewed to determine if newer compensating controls or subsequent patches can address vulnerabilities that were previously accepted, or if conditions have changed, increasing the risk.	●	○	●	◐	○
4.8	Establish a process to risk-rate vulnerabilities based on the exploitability and potential impact of the vulnerability, and segmented by appropriate groups of assets (example, DMZ servers, internal network servers, desktops, laptops). Apply patches for the riskiest vulnerabilities first. A phased rollout can be used to minimize the impact to the organization. Establish expected patching timelines based on the risk rating level.	●	○	●	n/a	○

○ = Not implemented ◐ = Partially Implemented ● = Fully Implemented n/a = Not Applicable

Another area we evaluated was the agency's processes for patching systems to prevent vulnerabilities and for identifying and remediating vulnerabilities that are detected. Vulnerability management is a joint effort between PERS and the Enterprise Security Office within the Office of the State Chief Information Officer. We found PERS generally has formal policies in place for vulnerability management. PERS has also partially implemented automated controls for most of the related sub-controls. For example, the agency has implemented a tool, provided by the Enterprise Security Office, which scans each device on its network for vulnerabilities. It has established processes to prioritize the remediation of those vulnerabilities, but does not track vulnerabilities over time to ensure all identified vulnerabilities are remediated. The agency also uses a formalized reporting process to share the results of these scans with appropriate governance bodies.

Agencies should be continuously engaged in identifying, remediating, and minimizing security vulnerabilities to ensure their assets are safeguarded. Attackers commonly exploit IT systems that have not been patched with security updates or suffer other known vulnerabilities. By scanning the network for those known vulnerabilities, an organization can identify and prioritize software patching and other remediation activities to ensure these known risks are controlled. Attackers may exploit known vulnerabilities to compromise the confidentiality, integrity, or availability of agency data. Agency management should ensure processes are in place to keep informed of available patches, test those patches for compatibility on the agency's systems, document the basis for the decision to implement patches or not, and implement appropriate changes in a timely manner.

CIS Control™ 5: Controlled Use of Administrative Privileges

		Audit Results				
#	**CIS Critical Security Controls™, Sub-Controls v6.1** Controlled Use of Administrative Privileges	**Performed**	**Managed**	**Defined**	**Automated**	**Optimizing**
5.1	Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.	●	○	●	○	○
5.2	Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive.	●	n/a	◐	○	○
5.3	Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.	●	○	○	○	○
5.4	Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group, or when a new local administrator account is added on a system.	●	●	○	○	○
5.5	Configure systems to issue a log entry and alert on any unsuccessful login to an administrative account.	n/a	○	○	○	○
5.6	Use multifactor authentication for all administrative access, including domain administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards, certificates, One Time Password (OTP) tokens, biometrics, or other similar authentication methods.	○	○	○	○	○
5.7	Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).	n/a	○	◐	○	○
5.8	Administrators should be required to access a system using a fully logged and non-administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems.	○	○	○	○	○
5.9	Administrators shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.	○	○	○	○	○

○ = Not implemented ◐ = Partially Implemented ● = Fully Implemented n/a = Not Applicable

We also evaluated the agency's processes to grant and monitor privileged access, to log and monitor login activity, and to establish robust authentication procedures.[19] We found PERS generally lacked formal policies for this control. Furthermore, PERS generally lacked manual or automated procedures for controlling administrative privileges. We also noted the agency's minimum password length requirements for administrator accounts was set below state standards and that PERS does not proactively monitor administrator account activity.

Management should ensure that only authorized users are able to perform administrative functions on the agency's information systems. While some users may have authorization to

[19] Privileged access refers to the ability of some users to take actions that may affect computing systems, network communications, or the accounts, files, data, or processes of other users. Privileged access implies greater access than the average end user.

read, edit, or delete data based on their job duties, certain users have access to advanced functions such as system control, monitoring, or administrative functions. Actions performed under these administrative accounts may have critical effects on the agency's systems. Therefore, use of accounts with these privileges should be effectively controlled by management, which should implement controls to segregate, manage, and monitor use of these accounts.

Recommendations

To improve IT strategic planning practices, we recommend PERS:

1. Develop a detailed IT strategic plan that includes how IT resources will be managed to meet stated objectives.
2. Develop and implement a method to track staff time by task or project.
3. Implement comprehensive IT portfolio management including tracking and managing all IT projects and ongoing maintenance efforts.
4. Update documentation around core competencies and skillsets required for the Information Services Division, and clearly define their connection to strategic goals.
5. Establish a detailed plan to recruit, train, and retain quality IT staff.

To improve the agency's disaster recovery capability, we recommend PERS:

6. Develop a process to schedule, track, and allocate sufficient resources to completing the disaster recovery plan.
7. Ensure the disaster recovery plan reflects short-term and long-term recovery of all critical business systems, including documenting detailed recovery procedures, alternative disaster scenarios, and planned responses.
8. Establish an alternative backup site that is geographically distant from the primary storage location.
9. Establish a disaster recovery warm site as directed by the Legislature.
10. Test the fully developed disaster recovery plan by 2020.

To improve capability in the critical cybersecurity controls, we recommend PERS and the Office of the State Chief Information Officer work collaboratively, where appropriate, to:

11. Improve security management by clearly defining security roles, properly vetting all individuals before granting access to PERS's IT resources, and ensuring that all individuals receive sufficient security awareness training.
12. Remedy weaknesses with Critical Security Control #1 – Hardware Inventory – by further developing written policies and procedures, as well as continuing to mature the application of the new inventory tool.
13. Remedy weaknesses with Critical Security Control #2 – Software Inventory – by further developing written policies and procedures, implementing software whitelisting, and continuing to mature the application of the new inventory tool.
14. Remedy weaknesses with Critical Security Control #3 – Secure Configurations – through monitoring of configuration changes and by further developing written policies and procedures.
15. Remedy weaknesses with Critical Security Control #4 – Vulnerability Assessment – by ensuring that known vulnerabilities are tracked and remediated.
16. Remedy weaknesses with Critical Security Control #5 – Privileged Access – by implementing improved segregation of duties, monitoring of administrative accounts, and by further developing written policies and procedures.

Oregon

Kate Brown, Governor

Public Employees Retirement System
Headquarters:
11410 S.W. 68th Parkway, Tigard, OR
Mailing Address:
P.O. Box 23700
Tigard, OR 97281-3700
888-320-7377
TTY (503) 603-7766
www.oregon.gov/pers

October 12, 2018

Kip Memmott, Director
Secretary of State, Audits Division
255 Capitol St. NE, Suite 500
Salem, OR 97310

Dear Mr. Memmott,

This letter provides a written response to the Audits Division's final draft audit report titled **Severe Deficiencies in Disaster Recovery Program and Insufficient Information Technology Planning Pose Substantial Risks to Beneficiaries and the State**.

Thank you for sharing an audit report regarding our Information Technology Strategic Planning Process as well as our Disaster Recovery Program. The Public Employees Retirement System (PERS) Executive Management appreciates the collaborative approach taken by the Audits Division and generally agrees with these findings.

The PERS Mission is to pay the right person, the right benefit, at the right time, and the functionality of our technology systems and disaster preparedness planning are key to that mission. We are committed to improving our capabilities in these areas, and have identified opportunities for improvements in recent years which this audit report validates. We are incorporating these practices as we hone our focus on strategic planning and communication with stakeholders about our continuing progress toward change.

PERS has already shifted in these areas from the point in time addressed in this audit. The agency is in process and anticipates implementation, of at least 13 of the 16 recommendations outlined in this report by June 30, 2019.

Those include: finalizing an Information Technology Strategic Plan with assistance from key stakeholders; focus on recruiting and retaining quality IT staff with appropriate skillsets for key projects; testing a fully developed disaster recovery plan that includes location of a warm site and off-site backup data storage; and a continued focus on information security including hardware, software, and data assets. Retirement system changes proposed during the 2019 legislative session may influence the proposed implementation dates for each recommendation.

We also appreciate this report highlighting a longer-term objective for the agency regarding enterprise portfolio management. PERS is in the initial stages of defining how to implement that methodology with appropriate processes and toolsets available to staff. We expect that new structure to be in place by June 30, 2020.

Fundamentally, PERS is committed to ensuring the safety and accessibility of data and technology resources, while balancing certain risks. An example of this is our focus on ensuring income continuity of retirees who already receive benefit payments. As part of our previously planned work, in August 2018, PERS engaged in a tabletop exercise with Oregon State Treasury to provide assurances to both parties that in the event of a local disaster, the Treasurer's office can re-run the monthly pension payroll on PERS' behalf. The exercise was a success and PERS is comfortable with taking on the risk of overpaying a very small (<1%) portion of total payroll as opposed to not paying the other 99% of payroll to over 145,000 members, thereby ensuring income continuity.

Below is our response to each recommendation in the audit. Given the balance required to implement the 16 recommendations alongside the agency's current workload, PERS has charted a multi-year effort to address the recommendations using a risk appetite and mitigation approach. We look forward to sharing our successes with stakeholders over the next year and appreciate the opportunity to highlight the progress to date in addressing some of these recommendations.

RECOMMENDATION 1 Develop a detailed IT Strategic Plan that includes how IT resources will be managed to meet stated objectives.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 6 months)**	**Name and phone number of specific point of contact for implementation**
Agree	6/30/2019	Jordan Masanga (503)603-7702

Narrative for Recommendation 1

Agreed. The IT Strategic Plan exists and management will collaborate with the business to improve the Plan to ensure better alignment and communication, including how IT resources will be managed.

RECOMMENDATION 2 Develop and implement a method to track staff time by task or project.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 6 months)**	**Name and phone number of specific point of contact for implementation**
Agree	6/30/2020	Yvette Elledge-Rhodes (503)603-7685 & Jordan Masanga (503)603-7702

Narrative for Recommendation 2

Agreed. Management will enhance our methodology to track staff time by task or project.

RECOMMENDATION 3
Implement comprehensive IT portfolio management including tracking and managing all IT projects and ongoing maintenance efforts.

Agree or Disagree with Recommendation	Target date to complete implementation activities (Generally expected within 6 months)	Name and phone number of specific point of contact for implementation
Agree	6/30/2020	Yvette Elledge-Rhodes (503)603-7685 & Jordan Masanga (503)603-7702

Narrative for Recommendation 3
Agreed. Management will implement an agency-wide portfolio management program which will include enterprise-wide IT projects as well as ongoing maintenance efforts.

RECOMMENDATION 4
Update documentation around core competencies and skillsets required for the Information Services Division, and clearly define their connection to strategic goals.

Agree or Disagree with Recommendation	Target date to complete implementation activities (Generally expected within 6 months)	Name and phone number of specific point of contact for implementation
Agree	6/30/2019	Jordan Masanga (503)603-7702

Narrative for Recommendation 4
Agreed. Management will update core competencies and skillsets for the Information Services Division and tie these to PERS' strategic goals.

RECOMMENDATION 5
Establish a detailed plan to recruit, train, and retain quality IT staff.

Agree or Disagree with Recommendation	Target date to complete implementation activities (Generally expected within 6 months)	Name and phone number of specific point of contact for implementation
Agree	6/30/2019	Jordan Masanga (503)603-7702

Narrative for Recommendation 5
Agreed. Management will develop a detailed workforce development plan as set forth in the 5-year IT Strategic Plan.

<table>
<tr><td colspan="3"><b>RECOMMENDATION 6</b>
Develop a process to schedule, track, and allocate sufficient resources to completing the disaster recovery plan.</td></tr>
<tr><th>Agree or Disagree with Recommendation</th><th>Target date to complete implementation activities (Generally expected within 6 months)</th><th>Name and phone number of specific point of contact for implementation</th></tr>
<tr><td>Agree</td><td>6/30/2019</td><td>Jason Stanley
(503)603-7504</td></tr>
</table>

Narrative for Recommendation 6

Agreed. Management will develop a detailed Project Plan to ensure resources are sufficient to complete the disaster recovery plan by the end of the 2017-2019 biennium.

<table>
<tr><td colspan="3"><b>RECOMMENDATION 7</b>
Ensure the disaster recovery plan reflects short-term and long-term recovery of all critical business systems, including documenting detailed recovery procedures, alternative disaster scenarios, and planned responses.</td></tr>
<tr><th>Agree or Disagree with Recommendation</th><th>Target date to complete implementation activities (Generally expected within 6 months)</th><th>Name and phone number of specific point of contact for implementation</th></tr>
<tr><td>Agree</td><td>6/30/2019</td><td>Jason Stanley
(503)603-7504</td></tr>
</table>

Narrative for Recommendation 7

Agreed. Management will develop a disaster recovery plan which will recover all critical business systems, necessary to meet both the statutory requirements and those business systems deemed critical by PERS executive leadership team.

<table>
<tr><td colspan="3"><b>RECOMMENDATION 8</b>
Establish an alternative backup site that is geographically distant from the primary storage location.</td></tr>
<tr><th>Agree or Disagree with Recommendation</th><th>Target date to complete implementation activities (Generally expected within 6 months)</th><th>Name and phone number of specific point of contact for implementation</th></tr>
<tr><td>Agree</td><td>6/30/2019</td><td>Jordan Masanga
(503)603-7702</td></tr>
</table>

Narrative for Recommendation 8

Agreed. Management will establish an alternative backup site outside the primary storage location via a Cloud solution.

RECOMMENDATION 9
Establish a disaster recovery warm site as directed by the Legislature.

Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 6 months)**	**Name and phone number of specific point of contact for implementation**
Agree	6/30/2019	Jordan Masanga (503)603-7702

Narrative for Recommendation 9
Agreed. Management will establish a disaster recovery warm site by the end of the 2017-2019 biennium via a Cloud solution.

RECOMMENDATION 10
Test the fully developed disaster recovery plan by 2020.

Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 6 months)**	**Name and phone number of specific point of contact for implementation**
Agree	6/30/2019	Jason Stanley (503)603-7504

Narrative for Recommendation 10
Agreed. Management will develop and test its disaster recovery plan by the end of the 2017-2019 biennium.

RECOMMENDATION 11
Improve security management by clearly defining security roles, properly vetting all individuals before granting access to PERS' IT resources, and ensuring that all individuals receive sufficient security awareness training.

Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 6 months)**	**Name and phone number of specific point of contact for implementation**
Agree	6/30/2019	Jason Stanley (503)603-7504

Narrative for Recommendation 11
Agreed. Management will clearly define its security roles, and vet all individuals prior to granting access to PERS' IT resources. Furthermore, management will ensure agency staff receive sufficient security awareness training.

RECOMMENDATION 12 Remedy weaknesses with Critical Security Control #1 – Hardware Inventory – by further developing written policies and procedures, as well as continuing to mature the application of the new inventory tool.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 6 months)**	**Name and phone number of specific point of contact for implementation**
Agree	6/30/2019	Jason Stanley (503)603-7504

Narrative for Recommendation 12
Agreed. Management will strengthen its hardware inventory controls to remedy its perceived weaknesses with CSC #1.

RECOMMENDATION 13 Remedy weaknesses with Critical Security Control #2 – Software Inventory – by developing written policies and procedures, implementing software whitelisting, and continuing to mature the application of the new inventory tool.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 6 months)**	**Name and phone number of specific point of contact for implementation**
Agree	6/30/2019	Jason Stanley (503)603-7504

Narrative for Recommendation 13
Agreed. Management will strengthen its software inventory controls to remedy its perceived weaknesses with CSC #2. Furthermore, PERS will evaluate the use of software whitelisting based on its risk to the agency. If, after a risk analysis categorizes this as a high risk, PERS will implement software whitelisting controls.

RECOMMENDATION 14 Remedy weaknesses with Critical Security Control #3 – Secure Configurations – through monitoring of configuration changes and by developing written policies and procedures.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 6 months)**	**Name and phone number of specific point of contact for implementation**
Agree	6/30/2019	Jason Stanley (503)603-7504

Narrative for Recommendation 14
Agreed. Management will strengthen its secure configuration controls to remedy its perceived weaknesses with CSC #3.

RECOMMENDATION 15
Remedy weaknesses with Critical Security Control #4 – Vulnerability Assessment – by ensuring that known vulnerabilities are tracked and remediated.

Agree or Disagree with Recommendation	Target date to complete implementation activities (Generally expected within 6 months)	Name and phone number of specific point of contact for implementation
Agree	6/30/2019	Jason Stanley (503)603-7504

Narrative for Recommendation 15
Agreed. Management will strengthen its vulnerability management program by ensuring known vulnerabilities are tracked and remediated in accordance with the agency and statewide standards.

RECOMMENDATION 16
Remedy weaknesses with Critical Security Control #5 – Privileged Access – by implementing improved segregation of duties, monitoring of administrative accounts, and developing additional written policies and procedures.

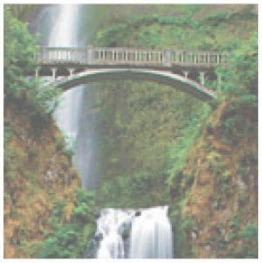
Agree or Disagree with Recommendation	Target date to complete implementation activities (Generally expected within 6 months)	Name and phone number of specific point of contact for implementation
Agree	12/31/2019	Jason Stanley (503)603-7504

Narrative for Recommendation 16
Agreed. Currently PERS does not have personnel which can be segregated from its IT Team and monitor administrative accounts. Therefore, Management will improve its privileged access controls once sufficient resources have been granted and the position(s) filled. In the meantime, PERS will work to strengthen CSC #5 through administrative controls (i.e., policies, standards, and procedures.)

Please contact Kevin Olineck, Director at (503) 603-7695 with any questions.

Sincerely,

Kevin Olineck,
Director



Audit Team

Will Garber, CGFM, MPA, Deputy Director

Teresa Furnish, CISA, Audit Manager

Ian Green, M.Econ, CGAP, CFE, Principal Auditor

Sherry Kurk, CISA, Staff Auditor

About the Secretary of State Audits Division

The Oregon Constitution provides that the Secretary of State shall be, by virtue of his office, Auditor of Public Accounts. The Audits Division performs this duty. The division reports to the elected Secretary of State and is independent of other agencies within the Executive, Legislative, and Judicial branches of Oregon government. The division has constitutional authority to audit all state officers, agencies, boards and commissions as well as administer municipal audit law.

This report is intended to promote the best possible management of public resources.
Copies may be obtained from:

Oregon Audits Division
255 Capitol St NE, Suite 500 | Salem | OR | 97310

(503) 986-2255
sos.oregon.gov/audits